

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 10/816,791
Filed: **APRIL 2, 2004**

In the Claims:

Claims 1-11 (Cancelled).

12. (Currently Amended) A method for generating output bytes corresponding to respective input bytes according to a one-to-one binary function representing a cryptographic algorithm, the method comprising:

decoding an input byte and generating at least one bit string that contains only one active bit, with the decoding comprising subdividing the input byte into a left nibble and a right nibble, and decoding the left nibble and right nibble into a left 16-bit string and a right 16-bit string, respectively, each 16-bit string containing only one active bit;

using an array of logic gates for logically combining the 16-bit strings ~~bits of the at least one bit string~~ according to the one-to-one binary function and generating a an encrypted 256-bit string without the use of a lookup table; and

encoding the encrypted 256-bit string for obtaining an output byte for the cryptographic algorithm.

Claims 13 and 14 (Cancelled).

15. (Previously Presented) A method according to Claim 12, wherein the one-to-one binary function represents a ByteSub operation of a Rijndael AES encryption/decryption algorithm.

16. (Previously Presented) A method according to Claim

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 10/816,791
Filed: **APRIL 2, 2004**

13, wherein the array of logic gates comprises AND gates, with each bit of the 256-bit string being obtained by ANDing among the bits of the 16-bit strings.

17. (Currently Amended) A method for implementing a cryptographic algorithm comprising:

decoding an input byte and generating at least one bit string that contains only one active bit, with the decoding comprising subdividing the input byte into a left nibble and a right nibble, and decoding the left nibble and right nibble into a left string and a right string, respectively, each string containing only one active bit;

using an array of logic gates for logically combining the bit strings ~~bits of the at least one bit string~~ according to the one-to-one binary function and generating a an encrypted bit string without the use of a lookup table; and

encoding encrypted the bit string for obtaining an output byte for the cryptographic algorithm.

18. (Previously Presented) A method according to Claim 17, wherein the cryptographic algorithm comprises a Rijndael AES encryption/decryption algorithm.

19. (Previously Presented) A method according to Claim 18, wherein the one-to-one binary function represents a ByteSub operation in the Rijndael AES encryption/decryption algorithm.

Claims 20 and 21 (Cancelled).

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 10/816,791
Filed: **APRIL 2, 2004**

22. (Previously Presented) A method according to Claim 20, wherein the array of logic gates comprises AND gates, with each bit of the bit string being obtained by ANDing among the bits of the 16-bit strings.

23. (Currently Amended) A device for implementing a cryptographic algorithm, the device comprising:

 a decoder for decoding an input byte and generating at least one bit string that contains only one active bit, said decoder comprising a left decoder being input with a left nibble of the input byte and a right decoder being input with a right nibble of the input byte, and decoding the left nibble and right nibble into a left 16-bit string and a right 16-bit string, respectively, each 16-bit string containing only one active bit;

 an array of logic gates being input with the 16-bit strings ~~at least one bit string~~, and generating a an encrypted 256-bit string without the use of a lookup table by logically combining the 16-bit strings ~~bits of the at least one bit string~~ according to the one-to-one binary function; and

 an encoder being input with the encrypted 256-bit string and generating an output byte for the cryptographic algorithm.

Claim 24 (Cancelled).

25. (Currently Amended) A device according to ~~Claim 24~~ Claim 23, wherein said array of logic gates comprises an array of 256 AND gates, each AND gate generating a respective bit of the

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 10/816,791
Filed: **APRIL 2, 2004**

encrypted 256-bit string by ANDing bits of the 16-bit strings.

26. (Currently Amended) A device according to ~~Claim 24~~
Claim 23, further comprising:

an array of multiplexers each being input with bits of the 16-bit strings and being driven by selection signals, and generating a respective intermediate bit being fed to said array of logic gates; and

said array of logic gates generating bits of the encrypted 256-bit string by logically combining the intermediate bits.

Claim 27 (Cancelled).

28. (Currently Amended) A cryptographic device for implementing a cryptographic algorithm, the cryptographic device comprising:

a decoder for decoding an input byte and generating at least one bit string that contains only one active bit, said decoder comprising a left decoder being input with a left nibble of the input byte and a right decoder being input with a right nibble of the input byte, and decoding the left nibble and right nibble into a left 16-bit string and a right 16-bit string, respectively, each 16-bit string containing only one active bit;

an array of logic gates being input with the 16-bit strings ~~at least one bit string~~, and generating a an encrypted 256-bit string without the use of a lookup table by logically combining the 16-bit strings ~~bits of the at least one bit string~~ according to

In re Patent Application of:
MACCHETTI ET AL.
Serial No. 10/816,791
Filed: **APRIL 2, 2004**

a one-to-one binary function; and
an encoder being input with the encrypted 256-bit string
and generating an output byte for the cryptographic algorithm.

29. (Previously Presented) A cryptographic device
according to Claim 28, wherein the cryptographic algorithm
comprises a Rijndael AES encryption/decryption algorithm.

30. (Previously Presented) A cryptographic device
according to Claim 29, wherein the one-to-one function
corresponds to a Bytesub operation within the Rijndael AES
encryption/decryption algorithm.

Claim 31 (Cancelled).

32. (Currently Amended) A cryptographic device
according to ~~Claim 31~~ Claim 28, wherein said array of logic gates
comprises an array of 256 AND gates, each AND gate generating a
respective bit of the encrypted 256-bit string by ANDing bits of
the 16-bit strings.

33. (Currently Amended) A cryptographic device
according to ~~Claim 31~~ Claim 28, further comprising:
an array of multiplexers each being input with bits of
the 16-bit strings and being driven by selection signals, and
generating a respective intermediate bit being fed to said array of
logic gates; and
said array of logic gates generating bits of the

In re Patent Application of:

MACCHETTI ET AL.

Serial No. 10/816,791

Filed: **APRIL 2, 2004**

_____/

encrypted 256-bit string by logically combining the intermediate bits.

Claim 34 (Cancelled).